CLAIMS

We claim:

1. A processing system comprising:

an application device that is configured to communicate information with a physical-layer access device via a link-layer access device,

a node controller that is configured to control the link-layer access device,

the link-layer access device, operably coupled to the application device, the node controller, and the physical-layer access device, that is configured to facilitate an exchange of the information from and to the application device with data that is communicated to and from the physical-layer access device;

wherein,

the link-layer access device is further configured to provide, in response to one or more commands from the node controller, one or more cryptographic items based on one or more parameters from the node controller.

2. The processing system of claim 1, wherein

the one or more cryptographic items include at least one of:

a digital signature,

a verification of a digital signature, and

a cryptographic key item.

3. The processing system of claim 1, wherein

the one or more cryptographic items include:

a digital signature,

a verification of a digital signature, and

a cryptographic key item.

4. The processing system of claim 1, wherein

the link-layer access device includes a multiplication device that is configured to derive a second point on an elliptic curve from a first point on the elliptic curve, based on the one or more of the parameters from the node controller.

5. The processing system of claim 1, wherein

the node controller is configured to effect an exchange of a cryptographic key with an other processing system, and

the one or more cryptographic items from the link-layer access device includes the cryptographic key.

6. The processing system of claim 1, wherein

the commands from the node controller include: a basepoint multiply command, a point multiply command, an EC-DSA verify command, and an EC-DSA sign command.

7. A link-layer access device comprising:

an application-layer interface device that is configured to communicate information with an application-layer device,

a physical-layer interface device that is configured to communicate data with a physical-layer device,

a buffer device, operably coupled to the application-layer interface device and the physical-layer interface device, that is configured to facilitate an exchange of the information of the application-layer device and the data of the physical-layer device,

a controller interface device, operably coupled to the application-layer interface device and the physical-layer interface device, that is configured to facilitate control of the exchange of information and data, and

an accelerator, operably coupled to a controller via the controller interface device, that is configured to compute one or more cryptographic items, in response to one or more cryptographic commands from the controller, and to thereafter communicate the one or more cryptographic items to the controller.

8. The link-layer access device of claim 7, wherein

the accelerator includes a multiplication device that is configured to derive a second point on an elliptic curve from a first point on the elliptic curve, based on one or more of parameters provided by the controller.

9. The link-layer access device of claim 7, wherein

the one or more cryptographic items includes at least one of:

a signature of a message,

a verification of a digital signature,

a hash of one or more parameters,

a random number,

an exponentiation of one or more parameters, and

an elliptic curve multiplication of one or more parameters,

the one or more parameters being provided by the controller.

10. The link-layer access device of claim 7, wherein

the one or more cryptographic items include:

a signature of a message,

a verification of a digital signature, and

an elliptic curve multiplication of one or more parameters,

the one or more parameters being provided by the controller.

11. The link-layer access device of claim 7, wherein

the one or more cryptographic commands include: a basepoint multiply command, a point multiply command, an EC-DSA Verify command, and an EC-DSA sign command.

12. A method for communications comprising:

communicating information from and to an application device to and from a physical-layer access device via a link-layer access device,

controlling the link-layer access device, in dependence upon commands from a node controller,

effecting an exchange of the information from and to the application device with data that is communicated to and from the physical-layer access device, and

determining one or more cryptographic items via computations within the link-layer access device, based on one or more parameters that are provided to the link-layer access device by the node controller.

13. The method of claim 12, wherein

the one or more cryptographic items include at least one of:

a digital signature,

a verification of a digital signature, and

a cryptographic key item.

14. The method of claim 12, wherein

the one or more cryptographic items include:

a digital signature,

a verification of a digital signature, and

a cryptographic key item.

15. The method of claim 12, wherein

determining the one or more cryptographic items includes

deriving a second point on an elliptic curve from a first point on the elliptic curve, based on the one or more of the parameters from the node controller.

15. The method of claim 12, further including

effecting an exchange of a cryptographic key with an other processing system, wherein

the one or more cryptographic items from the link-layer access device includes the cryptographic key.

16. The method of claim 12, wherein

the commands from the node controller include: a basepoint multiply command, a point multiply command, an EC-DSA verify command, and an EC-DSA sign command.